REMARKS

Applicants appreciate the Examiner's thorough review and consideration of the subject application. The non-final Office Action of August 19, 2004 has been received and its contents carefully noted. Claims 1-10 are currently pending in the application. By this amendment, claims 1, 5, 8, and 9 have been amended, and new claim 10 has been added. No new matter has been added. Thus, the amendments should be entered in to the record. The Examiner is respectfully invited to pass claims 1-10 to allowance for the reasons noted below.

35 U.S.C. § 102 Rejection

Claims 1-3 and 5-8 are rejected under 35 U.S.C. § 102(b) as being anticipated by U. S. Patent No. 5,826,014A issued to Coley, *et al.* ("Coley"). This rejection is respectfully traversed.

The claimed invention is directed to a method and system used to protect a web server against attack. In one embodiment, the method instructs the protective equipment for a web server to pass the received message to the web server, regardless of an ongoing attack, when the source address of the received message matches an address contained in the database of privileged source addresses. In the system, logic is provided for, when the source address of the received message appears in the database of privileged source addresses, instructing protective equipment to pass the received message to a web server, regardless of an ongoing attack. In another embodiment, the system includes a database of privileged source addresses, which permits a packet containing a privileged source address to pass to the web server regardless of an ongoing attack.

Coley does not teach these features. Coley discloses a method for improving the operation of equipment used to protect a web server against attack. But, in contrast to the claimed invention, Coley discloses a firewall comprised of a plurality of "proxy agents," each of which is assigned to a particular "port." Each agent monitors its assigned port and compares the source addresses of received packets with an authorized list. Packets having source addresses that do not appear on the authorized list are discarded, as are packets having source addresses that appear on a non-authorized list. Packets whose source addresses match those on the authorized list are subjected to a pre-determined set of verification tests. However, after this stage, only those packets which successfully pass the entire set of verification tests are passed to the web server. Coley would thus suggest that the received message would not pass to the web server, when under attack, because the message would not pass through the verification tests.

Thus, in the claimed invention, the privileged source addresses of the invention are designated so that messages containing source addresses that match those in the database are passed to the web server regardless of an ongoing denial-of-service, or other, attack. In contrast, Coley's proxy agents directly connect an incoming request with a destination host machine, only when it is known that the source is inherently secure. As Coley suggests, this might occur where a firewall protected machine at a company headquarters communicates with the company's R & D site. An attack against a company webserver, however, is not likely to originate at one of the company's firewall protected machines. Consequently, this example demonstrates that Coley connects an incoming request directly to a destination host machine only at times when the sending machine is not attacking (e.g., no attack is ongoing).

Claim 5 also recites the database of privileged source addresses, a feature not disclosed by Coley. For these reasons, claims 1 and 5 are allowable over Coley. Accordingly, allowance of claims 1 and 5, and their respective dependent claims 2-4 and 6-7 is respectfully requested.

35 U.S.C. § 103 Rejection

Claims 4 and 9 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Coley in view of U. S. Patent No. 6,363,489A issued to Comay, et al. ("Comay"). This rejection is respectfully traversed.

The Examiner admits Coley does not disclose adding the source address of the received message to the database of blocked source addresses, and does not disclose blocking subsequent messages that bear the source address of the received message (e.g., two features of claims 4 and 9). However, the Examiner argues that it would have been obvious to modify the teachings of Coley with the teachings of Comay in order to update Coley's list of unauthorized sources. *See* Office Action, page 10, paragraphs 1 and 2. The Examiner further suggests that such a combination would result in the claimed invention. *Id.* Applicants, however, offer the following remarks in traversal of these arguments.

The automatic intrusion detection system and method disclosed by Comay are made possible by providing a "marker" (e.g., false information) to an unauthorized user who gathers information from and about the webserver prior to an attack. The marker is designed so that any subsequent attempt of the unauthorized user to use the false data will automatically identify the unauthorized user as hostile. Comay discloses the use of an intruder database to store hostile or unauthorized source addresses. Comay further discloses adding a source address to the intruder database, but only after a scan is detected or a destination address appears in a marker database.

However, the claimed invention differs from Comay in that the method of the present invention does not use a marker, and does not check incoming packets to determine whether they are capable of performing scan operations. In contrast, embodiments of the invention check a database of privileged source addresses; check a database of blocked source addresses (if the source address of a received message does not appear in the database of privileged source addresses); and add the source addresses of the received message to the database of blocked source addresses when the source address of the received message does not appear in the database of blocked source addresses.

Moreover, even if the teachings of Coley and Comay were combined, they would fail to disclose the invention as claimed. Instead, the resultant combination would most likely yield a proxy-based firewall server (Coley) that analyzes received packets to determine whether each packet is capable of scanning to probe for possibly vunerable services in the network (Comay). Each time such a packet was detected, the modified proxy-based firewall (Coley) would attach a marker to the return packet (Comay). Thereafter, the modified firewall server would consider hostile any received packet that contained the marker, and appropriate security measures would be taken. Additionally, once a scanning packet was detected, the source address of the packet would be added to an intruder database (Comay). If a packet had no scanning capability, its destination address would be compared to a marker database (Comay), and if found therein, the packet's source address would be added to the intruder database. However, nothing in this combination discloses the database of privileged source addresses or other features of claims 4 and 9 (Comay).

Accordingly, allowance of claims 4 and 9 is respectfully requested.

Added Claims

Added claim 10 is allowable by virtue of its dependency from allowable claim 1. Claim 10 is further allowable because neither Coley nor Comay, alone or in combination, disclose or suggest:

- detecting cessation of the attack;
- removing one or more source addresses used by an attacker from a database of blocked source addresses; and
- unblocking the one or more source addresses just removed.

Accordingly, allowance of new claim 10 is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants submit that all of the objections and rejections have been overcome, and that the claims are patentably distinct from the prior art of record and in condition for allowance. The Examiner is respectfully requested to pass the above application to issue, and to contact the undersigned at the telephone number listed below, if needed. Applicants hereby make a written conditional petition for extension of time, if required. Please charge any deficiencies in fees and credit any overpayment of fees to **Deposit Account No. 09-0457** (Endicott).

Respectfully submitted,

Andrew M. Calderon
Reg. No. 38,093

Jonathan Thomas
Reg. No. 50,352

McGuireWoods LLP
1750 Tysons Boulevard
Suite 1800
McLean, VA 22102-4215
Tel: 703-712-5426
Fax: 703-712-5285